(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－332742
（P2000－332742A）
(43)公開日　平成12年11月30日(2000.11.30)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
H04L	9/08		H04L	9/00	601A　5B017
G06F	12/14	320	G06F	12/14	320E　5D044
					320B　5J104
G09C	1/00	640	G09C	1/00	640Z　9A001
G11B	20/10		G11B	20/10	H

審査請求　未請求　請求項の数４　ＯＬ　（全　９　頁）　最終頁に続く

(21)出願番号　特願平11－136695

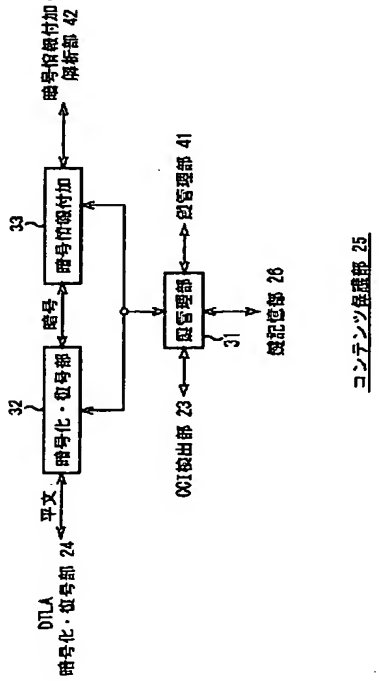
(22)出願日　平成11年５月18日(1999.5.18)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　濱田　一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　藪井　麻子
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

(54)【発明の名称】　情報処理装置および方法、並びに提供媒体

(57)【要約】
【課題】　コンテンツの不正利用を抑止する。
【解決手段】　鍵管理部３１は、アプリケーションが有する認証鍵Ｋｎが正規のものであるかを判定し、正規のものであると判定したときだけ、アプリケーションとのコンテンツの授受を実行するように、コンテンツ保護部２５を制御する。暗号化・復号部３２は、復号されているコンテンツを、鍵管理部３１から入力される暗号鍵Ｋｃを用いて暗号化し、暗号情報付加部３３に出力する。暗号情報付加部３３は、暗号化・復号部３２からの暗号化されたコンテンツに、暗号情報を付加して、アプリケーションに出力する。



【特許請求の範囲】
【請求項１】　著作権情報が付加されているコンテンツを編集可能であり、かつ、認証鍵および秘密鍵を有するアプリケーションプログラムを実行する情報処理装置において、
入力される前記コンテンツに付加されている前記著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成手段と、
前記暗号鍵を用いて前記コンテンツを暗号化する暗号化手段と、
前記アプリケーションプログラムから入力される前記認証鍵を用いて前記アプリケーションプログラムの正当性を判定する判定手段と、
前記アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成手段と、
前記秘密鍵生成手段が生成した前記秘密鍵を用いて暗号化した前記暗号鍵、および前記暗号化手段により暗号化された前記コンテンツを、前記判定手段の判定結果に対応して、前記アプリケーションプログラムに供給する供給手段とを含むことを特徴とする情報処理装置。
【請求項２】　前記判定手段は、リボケーションリストを参照することにより前記認証鍵の正当性を判定することを特徴とする請求項１に記載の情報処理装置。
【請求項３】　著作権情報が付加されているコンテンツを編集可能であり、かつ、認証鍵および秘密鍵を有するアプリケーションプログラムを実行する情報処理装置の情報処理方法において、
入力される前記コンテンツに付加されている前記著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成ステップと、
前記暗号鍵を用いて前記コンテンツを暗号化する暗号化ステップと、
前記アプリケーションプログラムから入力される前記認証鍵を用いて前記アプリケーションプログラムの正当性を判定する判定ステップと、
前記アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成ステップと、
前記秘密鍵生成ステップで生成した前記秘密鍵を用いて暗号化した前記暗号鍵、および前記暗号化ステップで暗号化した前記コンテンツを、前記判定ステップの判定結果に対応して、前記アプリケーションプログラムに供給する供給ステップとを含むことを特徴とする情報処理方法。
【請求項４】　著作権情報が付加されているコンテンツを編集可能であり、かつ、認証鍵および秘密鍵を有するアプリケーションプログラムを実行する情報処理装置に、
入力される前記コンテンツに付加されている前記著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成ステップと、
前記暗号鍵を用いて前記コンテンツを暗号化する暗号化ステップと、
前記アプリケーションプログラムから入力される前記認証鍵を用いて前記アプリケーションプログラムの正当性を判定する判定ステップと、
前記アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成ステップと、
前記秘密鍵生成ステップで生成した前記秘密鍵を用いて暗号化した前記暗号鍵、および前記暗号化ステップで暗号化した前記コンテンツを、前記判定ステップの判定結果に対応して、前記アプリケーションプログラムに供給する供給ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報処理装置および方法、並びに提供媒体に関し、特に、コンテンツの不正利用を抑止する場合に用いて好適な情報処理装置および方法、並びに提供媒体に関する。
【０００２】
【従来の技術】従来、著作権が保護されているコンテンツ（例えば、CD(Compact Disc)に記録されているオーディオデータ、DVD(Digital Versatile Disc)に記録されているAVデータ等）が不正に複製されることを抑止するために、コンテンツを記録可能な装置（例えば、MD(Mini Disc)レコーダ、CD-Rレコーダ、DV(Digital Video)レコーダ等）には、SCMS(Serial Copy Management System)、またはCGMS(Copy Generation Management System)が採用されている。SCMSやCGMSにおいては、コンテンツに所定の情報を付加し、その情報に基づいてコピー可能な回数を制限している。
【０００３】また、最近、コンテンツを再生、または記録するAV装置とパーソナルコンピュータとの間で、IEEE1394バスを介してコンテンツを通信することが可能となった。さらに、パーソナルコンピュータにおいては、CPU(Central Processing Unit)の高速化やハードディスクの大容量化にともない、上述したコンテンツを再生し、記録し、さらに編集することが可能となった。
【０００４】
【発明が解決しようとする課題】したがって、パーソナルコンピュータに、上述したコンテンツに付加されている情報を意図的に改ざんするような不正なアプリケーションプログラムがインストールされている場合、コンテンツが違法にコピーされてしまうことを抑止できない課題があった。
【０００５】本発明はこのような状況に鑑みてなされたものであり、パーソナルコンピュータにおいて、アプリケーションプログラムに供給される直前のコンテンツを暗号化することにより、不正なアプリケーションプログ

ラムを用いたコンテンツの不正利用を抑止できるようにするものである。

【０００６】

【課題を解決するための手段】請求項１に記載の情報処理装置は、入力されるコンテンツに付加されている著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成手段と、暗号鍵を用いてコンテンツを暗号化する暗号化手段と、アプリケーションプログラムから入力される認証鍵を用いてアプリケーションプログラムの正当性を判定する判定手段と、アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成手段と、秘密鍵生成手段が生成した秘密鍵を用いて暗号化した暗号鍵、および暗号化手段により暗号化されたコンテンツを、判定手段の判定結果に対応して、アプリケーションプログラムに供給する供給手段とを含むことを特徴とする。

【０００７】請求項３に記載の情報処理方法は、入力されるコンテンツに付加されている著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成ステップと、暗号鍵を用いてコンテンツを暗号化する暗号化ステップと、アプリケーションプログラムから入力される認証鍵を用いてアプリケーションプログラムの正当性を判定する判定ステップと、アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成ステップと、秘密鍵生成ステップで生成した秘密鍵を用いて暗号化した暗号鍵、および暗号化ステップで暗号化したコンテンツを、判定ステップの判定結果に対応して、アプリケーションプログラムに供給する供給ステップとを含むことを特徴とする。

【０００８】請求項４に記載の提供媒体は、入力されるコンテンツに付加されている著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成ステップと、暗号鍵を用いてコンテンツを暗号化する暗号化ステップと、アプリケーションプログラムから入力される認証鍵を用いてアプリケーションプログラムの正当性を判定する判定ステップと、アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成ステップと、秘密鍵生成ステップで生成した秘密鍵を用いて暗号化した暗号鍵、および暗号化ステップで暗号化したコンテンツを、判定ステップの判定結果に対応して、アプリケーションプログラムに供給する供給ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【０００９】請求項１に記載の情報処理装置、請求項３に記載の情報処理方法、および請求項４に記載の提供媒体においては、入力されるコンテンツに付加されている著作権情報に対応するソース鍵を用いて暗号鍵が生成され、暗号鍵を用いてコンテンツが暗号化される。また、アプリケーションプログラムから入力される認証鍵を用いて秘密鍵が生成されて、アプリケーションプログラムの正当性が判定され、その判定結果に対応して、秘密鍵を用いて暗号化した暗号鍵、および暗号化されているコンテンツが、アプリケーションプログラムに供給される。

【００１０】

【発明の実施の形態】本発明を適用したパーソナルコンピュータの構成例について、図１を参照して説明する。このパーソナルコンピュータ(PC)１は、IEEE1394バス２を介して、コンテンツを扱うことが可能な機器（例えば、図１に示すようなDVレコーダ(DVR)３、セットトップボックス(STB)４、およびハードディスク(HDD)５等）と接続されている。なお、IEEE1394バス２を介して通信されるコンテンツは、CPTWG(CopyProtection Technical Working Group）で推奨されるライセンス管理会社DTLA(Digital Transmission Licensing Administrator)がライセンスする方式（以下、DTLA方式と記述する）に基づいて暗号化されている。

【００１１】パーソナルコンピュータ１は、バス１６を介して接続されている、IEEE1394インタフェース１１、CPU１２、RAM１３、ROM１４、およびハードディスク１５から構成される。IEEE1394インタフェース１１は、IEEE1394バス２を介して、他の機器（DVR３等）から入力されるコンテンツを、パーソナルコンピュータ１で起動されている、コンテンツに対して再生、記録、編集等が可能なアプリケーションプログラム（以下、起動されている、コンテンツに対して再生、記録、編集等が可能なアプリケーションプログラムを、単にアプリケーションと記述する）に供給する。また、IEEE1394インタフェース１１は、アプリケーションが処理したコンテンツを、IEEE1394バス２を介して他の機器に出力する。

【００１２】なお、アプリケーションプログラムは、ハードディスク１５に記憶されており、ROM１４に記憶されているBIOSに基づくCPU１２の制御によって、RAM１３に転送されて起動される。また、このアプリケーションプログラムに対しては、DTLAのような暗号システムの管理者から固有の認証鍵Ｋｎが与えられているが、この認証鍵Ｋｎを得るためには、アプリケーションプログラムの制作元、およびユーザが、著作権が保護されているコンテンツを不正に利用しない旨を契約書等で誓約する必要がある。また、本明細書においてシステムの用語は、複数の装置、手段などにより構成される全体的な装置を意味するものである。

【００１３】ここで、認証鍵Ｋｎには、IDとSignatureの対となる２値が含まれており、一方に所定の演算式を適用した結果が他方となっている。また、双方に所定の演算式を適用することにより、正しい対であることが確認できる。この所定の演算式を知っている、すなわち、認証鍵Ｋｎの正当性を判定できるのは、鍵管理部３１（図３）だけである。また、所定の演算式を、IDとSign

atureを用いた逆算により求めることは非常に困難であるので、事実上、認証鍵Ｋｎを偽造することは不可能である。

【００１４】図２は、IEEE1394インタフェース１１の詳細な構成例を示している。制御部２１は、IEEE1394インタフェース１１の各部を制御する。入出力部２２は、IEEE1394バス２から入力される、DTLA方式で暗号化されているコンテンツを受け付けてCCI(Copy Control Infomation)検出部２３に出力する。CCI検出部２３は、入出力部２２から入力されるコンテンツをDTLA暗号化・復号部２４に供給するが、その際、コンテンツのヘッダに記録されているCCI（２ビット）を検出して、制御部２１、DTLA暗号化・復号部２４、およびコンテンツ保護部２５に供給する。

【００１５】なお、CCIは、自身が付加されているコンテンツに対して許可されているコピーの制御を示す情報であり、００，１０，０１，１１の４種類のステートがある。CCIが００(Copy free)である場合、対応するコンテンツに対しては無制限回数のコピーが許可されていることを意味している。CCIのステートが１０(One Generator Copy Possible)である場合、対応するコンテンツに対しては１回だけコピーが許可されていることを意味している。CCIのステートが０１(No More Copy)である場合、対応するコンテンツは、CCIのステートが１０であるコンテンツを複製したもの（２世代目）であって、これに対してはコピーが許可されていないことを意味している。CCIのステートが１１(Never copy)である場合、対応するコンテンツに対してはコピーが許可されていないことを意味している。

【００１６】DTLA暗号化・復号部２４は、CCI検出部２３から入力されたDTLA方式で暗号化されているコンテンツを復号し、コンテンツ保護部２５に出力する。また、DTLA暗号化・復号部２４は、コンテンツ保護部２５から入力されるコンテンツを、DTLA方式の用いて暗号化して入出力部２２に出力する。なお、DTLA暗号化・復号部２４における暗号化および復号は、DTLA暗号化・復号部２４とコンテンツを出力した装置（DVR３等）の間における、DTLA方式で定義されている相互認証作業が終了した後に実行される。

【００１７】コンテンツ保護部２５は、DTLA暗号化・復号部２４から入力されるコンテンツを暗号化してアプリケーションに供給する。また、コンテンツ保護部２５は、アプリケーションから入力される、暗号化されているコンテンツを復号してDTLA暗号化・復号部２４に供給する。鍵記憶部２６は、コンテンツ保護部２５における暗号化処理に用いられるソース鍵Ｋｓを、CCIのステート毎に複数個記憶している。

【００１８】図３は、コンテンツ保護部２５の詳細な構成例を示している。鍵管理部３１は、アプリケーションの鍵管理部４１（図４）から入力される認証鍵Ｋｎが正規のものであるかを判定し、認証鍵Ｋｎが正規のものであると判定したときだけ、アプリケーションとのコンテンツの授受を実行するように、コンテンツ保護部２５の各部を制御する。

【００１９】すなわち、鍵管理部３１は、アプリケーションからの認証鍵Ｋｎに含まれるIDに所定の演算式を適用し、その結果が対応するSignatureと等しいか否かを判定し、演算結果がSignatureと等しい（認証鍵Ｋｎが正規のものである）と判定した場合、さらに、IDとSignatureに所定の演算式を適用することにより、正しい対であるか否かを判定し、正しい対であると判定した場合、CCI検出部２３から入力されるCCIのステートに対応するソース鍵Ｋｓを読み出し、ソース鍵Ｋｓおよび乱数を用いて暗号鍵Ｋｃを生成して、暗号化・復号部３２に供給する。なお、暗号鍵Ｋｃは、所定の周期（例えば、３０秒間乃至１２０秒間）毎に更新される。また、鍵管理部３１は、CCIのステートを、暗号鍵Ｋｃを更新する毎に暗号情報付加部３３に出力する。さらに、鍵管理部３１は、アプリケーションの鍵管理部４１から入力される認証鍵等の秘密鍵Ｋａ算出用情報に基づいて秘密鍵Ｋａを生成し、暗号鍵Ｋｃを秘密鍵Ｋａを用いて暗号化して鍵管理部４１に出力する。

【００２０】暗号化・復号部３２は、DTLA暗号化・復号部２４からの復号されているコンテンツを、鍵管理部３１からの暗号鍵Ｋｃを用いて暗号化し、暗号情報付加部３３に出力する。また、暗号化・復号部３２は、暗号情報付加部３３からの、暗号化されているコンテンツを復号してDTLA暗号化・復号部２４に出力する。

【００２１】暗号情報付加部３３は、暗号化・復号部３２からの暗号化されたコンテンツに、CCIのステート（２ビット）、暗号鍵Ｋｃが更新される毎に切り替えられるevenまたはodd（１ビット）の暗号情報を付加して、アプリケーションの暗号情報解析部４２（図４）に出力する。また、暗号情報付加部３３は、暗号情報解析部４２からの暗号化されたコンテンツを、暗号化・復号部３２に出力する。

【００２２】図４は、コンテンツに対し再生、記録、編集等が可能なアプリケーションの機能ブロック図を示している。鍵管理部４１は、アプリケーションプログラムに対して与えられている認証鍵Ｋｎを記憶しており、アプリケーションがコンテンツの授受を開始する前に、記憶している認証鍵Ｋｎを、秘密鍵Ｋａ算出用情報とともに、コンテンツ保護部２５の鍵管理部３１に出力する。また、鍵管理部４１は、暗号情報解析部４２から入力される、暗号情報に含まれる暗号鍵Ｋｃの更新を示す情報（evenまたはodd）が切り替えられたか否かを示す情報に対応して、鍵管理部３１からの秘密鍵Ｋａで暗号化されている暗号鍵Ｋｃを復号し、暗号化・復号部４３に出力する。

【００２３】暗号情報解析部４２は、暗号情報付加部３

３から入力される、暗号鍵Ｋｃで暗号化されているコンテンツを暗号化・復号部４３に出力し、付加されている暗号情報を鍵管理部４１に出力する。また、暗号情報解析部４２は、暗号化・復号部４３からの暗号化されたコンテンツを暗号情報付加部３３に出力する。

【００２４】暗号化・復号部４３は、暗号情報解析部４２からの入力される暗号鍵Ｋｃで暗号化されているコンテンツを、鍵管理部４１からの暗号鍵Ｋｃを用いて復号し、コンテンツ処理部４４に出力する。また、暗号化・復号部４３は、コンテンツ処理部４４から入力されるコンテンツを暗号化し、暗号情報解析部４２に出力する。

【００２５】コンテンツ処理部４４は、入力されたコンテンツに対して、ユーザの操作に対応する処理（再生、記録、または編集等）を実行する。なお、コンテンツ処理部４４には、暗号情報解析部４２が解析した暗号情報に含まれるCCIが供給されるので、コンテンツ処理部４４においては、CCIに反するような処理（制限回数を超えるコピー等）は実行されない。

【００２６】なお、IEEE1394インタフェース１１を１個のLSI(Large Scale Integrated circuit)で実現すれば、回路の途中から復号されたコンテンツを読み出すような不正行為を抑止することが可能となる。

【００２７】次に、アプリケーションにコンテンツを入力する処理について、図５のフローチャートを参照して説明する。この入力処理は、IEEE1394インタフェース１１にDTLA方式で暗号化されているコンテンツが入力され、そのCCIが、CCI検出部２３で検出されてコンテンツ保護部２５の鍵管理部３１に入力され、DTLA方式で暗号化されているコンテンツが、DTLA暗号化・復号部２４で復号されてコンテンツ保護部２５の暗号化・復号部３２に入力された後に実行される。

【００２８】ステップＳ１において、アプリケーションの鍵管理部４１は、コンテンツ入力の要求、記憶している認証鍵Ｋｎ、および秘密鍵Ｋａ算出用情報を出力し、それらを、コンテンツ保護部２５の鍵管理部３１が受け付ける。

【００２９】ステップＳ２において、鍵管理部３１は、鍵管理部４１からの認証鍵Ｋｎが正規のものであるか否かを判定し、認証鍵Ｋｎが正規のものであると判定した場合、ステップＳ３に進む。

【００３０】ステップＳ３において、鍵管理部３１は、CCIのステートに対応するソース鍵Ｋｓを鍵記憶部２６から読み出して、ソース鍵Ｋｓと乱数を用いて暗号鍵Ｋｃを生成し、暗号化・復号部３２に出力する。また、鍵管理部３１は、暗号鍵Ｋｃを更新するタイミングを計測するタイマを０にリセットする。

【００３１】ステップＳ４において、鍵管理部３１は、秘密鍵Ｋａ算出用情報を用いて秘密鍵Ｋａを生成し、さらに、秘密鍵Ｋａを用いて暗号鍵Ｋｃを暗号化し、アプリケーションの鍵管理部４１に出力する。鍵管理部４１は、暗号鍵Ｋｃを復号する。

【００３２】ステップＳ５において、暗号化・復号部３２は、DTLA暗号化・復号部２４からの復号されているコンテンツを、鍵管理部３１からの暗号鍵Ｋｃを用いて暗号化し、暗号情報付加部３３に出力する。

【００３３】ステップＳ６において、暗号情報付加部３３は、CCIのステート、暗号鍵Ｋｃの更新を示す情報（いまの場合、暗号鍵Ｋｃは更新されていないのでeven）から成る暗号情報を生成し、暗号化・復号部３２からの暗号化されたコンテンツに付加して、アプリケーションの暗号情報解析部４２に出力する。暗号情報解析部４２は、暗号情報に含まれる、暗号鍵Ｋｃの更新を示す情報が切り替えられているか否かを判定し、判定結果を鍵管理部４１に出力する。鍵管理部４１は、この判定結果に基づき、いまの暗号鍵Ｋｃを暗号化・復号部４３に供給する。暗号化・復号部４３は、暗号鍵Ｋｃを用いてコンテンツを復号し、コンテンツ処理部４４に出力する。

【００３４】ステップＳ７において、鍵管理部３１は、全てのコンテンツをコンテンツ保護部２５からアプリケーションに出力したか否かを判定し、全てのコンテンツを出力していないと判定した場合、ステップＳ８に進む。ステップＳ８において、鍵管理部３１は、自己のタイマを参照することにより、いまの暗号鍵Ｋｃが用いられている時間を検知し、その時間が所定時間（３０秒間乃至１２０秒間）を経過したか否かを判定する。いまの暗号鍵Ｋｃが用いられている時間が所定時間を経過していないと判定された場合、ステップＳ５に戻り、それ以降の処理が繰り返される。

【００３５】その後、ステップＳ８において、いまの暗号鍵Ｋｃの使用時間が所定時間を経過したと判定された場合、ステップＳ９に進む。ステップＳ９において、鍵管理部３１は、ソース鍵Ｋｓと、再度発生させた乱数を用いて暗号鍵Ｋｃを生成（更新）し、暗号化・復号部３２に出力する。また、鍵管理部３１は、自己のタイマを０にリセットする。

【００３６】その後、ステップＳ４に戻り、ステップＳ７で全てのコンテンツを出力したと判定されるまで、以降の処理が繰り返される。ただし、ステップＳ６で付加される暗号情報に含まれる、暗号鍵Ｋｃの更新を示す情報は、ステップＳ９で暗号鍵Ｋｃが更新されているのでevenからoddに切り替えられる。この暗号鍵Ｋｃの更新を示す情報に対応して、鍵管理部４１から暗号化・復号部３２に供給される暗号鍵Ｋｃも更新される。

【００３７】なお、ステップＳ２において、認証鍵Ｋｎが正規のものではないと判定された場合、ステップＳ１０に進む。ステップＳ１０において、鍵管理部３１は、アプリケーションの鍵管理部４１に対して、認証は不可能である旨を通知する。

【００３８】次に、アプリケーションで処理されたコン

テンツをIEEE1394バス２に出力する処理について、図６のフローチャートを参照して説明する。この出力処理は、アプリケーションのコンテンツ処理部４４において編集されたコンテンツが暗号化・復号部４３に入力された後に実行される。

【００３９】ステップＳ２１において、アプリケーションの鍵管理部４１は、コンテンツ出力の要求、記憶している認証鍵Ｋｎ、秘密鍵Ｋａ算出用情報、および出力するコンテンツに対して設定するCCIのステートを、コンテンツ保護部２５の鍵管理部３１に出力する。

【００４０】ステップＳ２２において、鍵管理部３１は、鍵管理部４１からの認証鍵Ｋｎが正規のものであるか否かを判定し、認証鍵Ｋｎが正規のものであると判定した場合、ステップＳ２３に進む。

【００４１】ステップＳ２３において、鍵管理部３１は、鍵管理部４１から入力されたCCIのステートに対応するソース鍵Ｋｓを鍵記憶部２６から読み出して、ソース鍵Ｋｓと乱数を用いて暗号鍵Ｋｃを生成し、暗号化・復号部３２に供給する。ステップＳ２４において、鍵管理部３１は、鍵管理部４１からの秘密鍵Ｋａ算出用情報を用いて秘密鍵Ｋａを生成し、さらに、秘密鍵Ｋａを用いて、ステップＳ２２で生成した暗号鍵Ｋｃを暗号化し、アプリケーションの鍵管理部４１に出力する。鍵管理部４１は、暗号鍵Ｋｃを復号して、暗号化・復号部４３に出力する。

【００４２】ステップＳ２５において、アプリケーションの暗号化・復号部４３は、鍵管理部４１からの暗号鍵Ｋｃを用いて、コンテンツ処理部４４から入力されたコンテンツを暗号化し、暗号情報解析部４２および暗号情報付加部３３を介して、暗号化・復号部３２に出力する。

【００４３】ステップＳ２６において、暗号化・復号部３２は、ステップＳ２３で鍵管理部３１から入力された暗号鍵Ｋｃを用いて、アプリケーション（暗号化・復号部４３）からの暗号化されたコンテンツを復号し、DTLA暗号化・復号部２４に出力する。

【００４４】ステップＳ２７において、DTLA暗号化・復号部２４は、コンテンツ保護部２５の暗号化・復号部３２から入力された復号されているコンテンツを、DTLA方式で暗号化し、入出力部２２に出力する。

【００４５】ステップＳ２８において、入出力部２２は、DTLA暗号化・復号部２４からのDTLA方式で暗号化されているコンテンツをIEEE1394バス２に出力する。

【００４６】なお、ステップＳ２２において、認証鍵Ｋｎが正規のものではないと判定された場合、ステップＳ２９に進む。ステップＳ２９において、鍵管理部３１は、アプリケーションの鍵管理部４１に対して、認証は不可能である旨を通知する。

【００４７】また、この出力処理においても、上述した入力処理と同様、周期的に暗号鍵Ｋｃを変更するようにしてもよい。

【００４８】以上のように、本実施の形態によれば、正規の認証鍵Ｋｎを持っているアプリケーションに対してだけ、IEEE1394インタフェース１１のコンテンツ保護部２５は、コンテンツの授受を行うようになさてれいる。しかしながら、コンテンツの違法コピー等を実行可能なアプリケーションが、何らかの方法により、正規の認証鍵Ｋｎを取得し、コンテンツが不正に利用されてしまうことも考えられる。そこで、本発明においては、認証鍵Ｋｎの正当性を判定するコンテンツ保護部２５の鍵管理部３１に、不正に使用された認証鍵Ｋｎが登録されているリボケーションリストを記憶させ、認証処理の際、鍵管理部３１は、認証鍵Ｋｎに含まれるIDとSignatureの整合性の判定に加えて、リボケーションリストとの照合を実行するようにして、リボケーションリストに登録されている認証鍵Ｋｎは、IDとSignatureが対となっていても正規なものであると判定されないようになされている。

【００４９】なお、このリボケーションリストに関しては、その最新のものをインターネットやIEEE1394バス２等のネットワークを介して、鍵管理部３１に配信する方法が考えられる。また、このリボケーションリストの利用方法としては、認証鍵Ｋｎを個々に登録する方法と、複数の認証鍵Ｋｎをまとめて登録する方法（例えば、認証鍵ＫｎのIDのMSB(Most Significant Bit)側の所定ビットを指定する等）が考えられる。複数の認証鍵Ｋｎをまとめて登録する方法により、例えば、特定のソフトウェアメーカ（認証鍵Ｋｎを取得する際に誓約した規約に対する違反が発覚したソフトウェアメーカ）が製作した全てのアプリケーションを、正規なものではないと判定させることが可能となる。

【００５０】また、コンテンツ保護部２５からアプリケーションへのコンテンツの出力を検知し、その回数をインターネット等を介して、コンテンツの著作権の所有者や暗号システムの管理者に通知するようにすれば、コンテンツや暗号システムを使用したことに対して、ユーザに課金することや、暗号システムの使用状況を把握することが可能となる。

【００５１】なお、本発明は、IEEE1394バスに伝送されるコンテンツのアイソクロナスパケットおよびアシンクロナスパケット、並びに、他の伝送媒体に伝送されるコンテンツのパケットに対して適用することが可能である。

【００５２】また、上記各処理を行うコンピュータプログラムは、磁気ディスク、CD-ROM等の情報記録媒体よりなる提供媒体のほか、インターネット、デジタル衛星などのネットワーク提供媒体を介してユーザに提供することができる。

【００５３】

【発明の効果】以上のように、請求項１に記載の情報処

理装置、請求項３に記載の情報処理方法、および請求項４に記載の提供媒体によれば、認証鍵を用いてアプリケーションプログラムの正当性を判定し、その判定結果に対応して、秘密鍵を用いて暗号化した暗号鍵、および暗号鍵で暗号化されているコンテンツを、アプリケーションプログラムに供給するようにしたので、コンテンツの不正利用を抑止することが可能となる。

【図面の簡単な説明】

【図１】本発明を適用したパーソナルコンピュータ１の構成例を示すブロック図である。

【図２】図１のIEEE1394インタフェース１１の構成例を示すブロック図である。

【図３】図２のコンテンツ保護部２５の構成例を示すブロック図である。

【図４】パーソナルコンピュータ１で起動されているアプリケーションの機能を示すブロック図である。

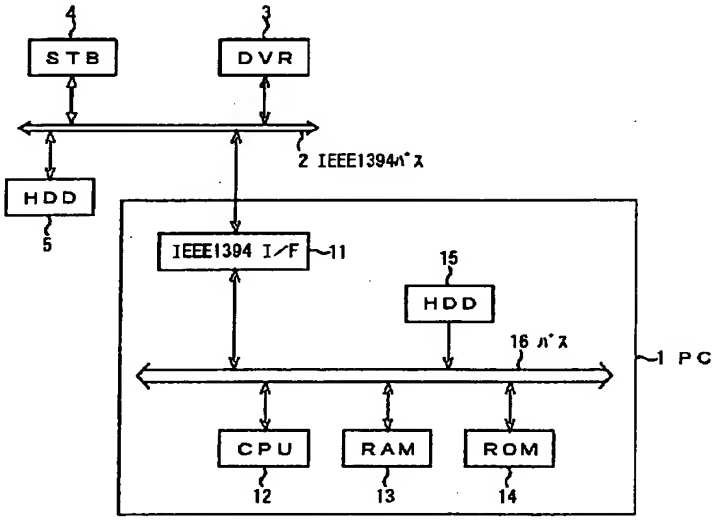
【図５】図１のIEEE1394インタフェース１１の動作を説明するフローチャートである。

【図６】図１のIEEE1394インタフェース１１の動作を説明するフローチャートである。

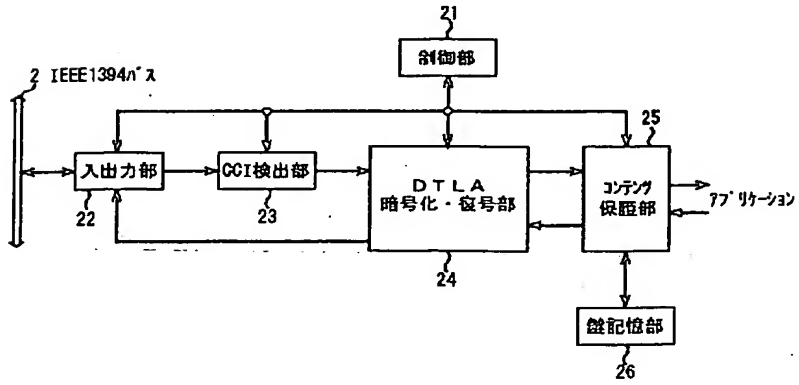
【符号の説明】

１　パーソナルコンピュータ，　２　IEEE1394バス，　１１　IEEE1394インタフェース，　２５　コンテンツ保護部，　３１　鍵管理部，　３２　暗号化・復号部，　３３　暗号情報付加部，　４１　鍵管理部，　４２　暗号情報解析部，４３　暗号化・復号部，　４４　コンテンツ処理部

【図１】

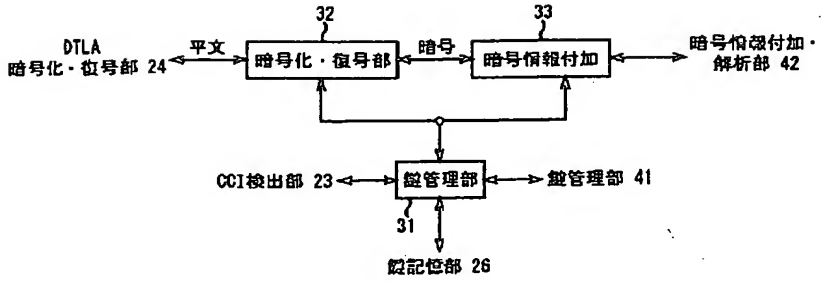


【図２】

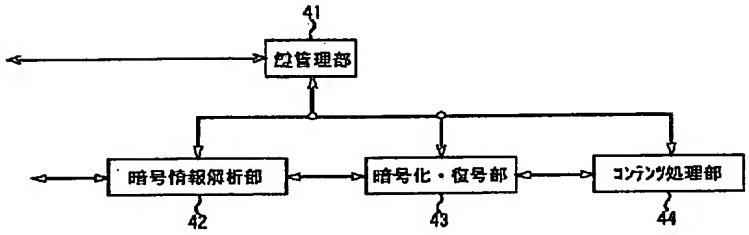


IEEE1394 I/F 11

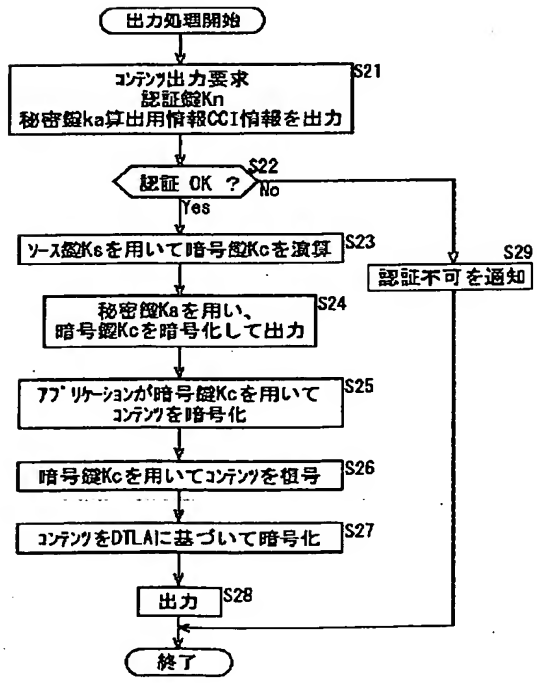
【図３】


32
33
DTLA
暗号化・復号部 24
平文
暗号化・復号部
暗号
暗号情報付加
暗号情報付加・
解析部 42
CCI検出部 23
鍵管理部
鍵管理部 41
31
認証部 26
コンテンツ保護部 25

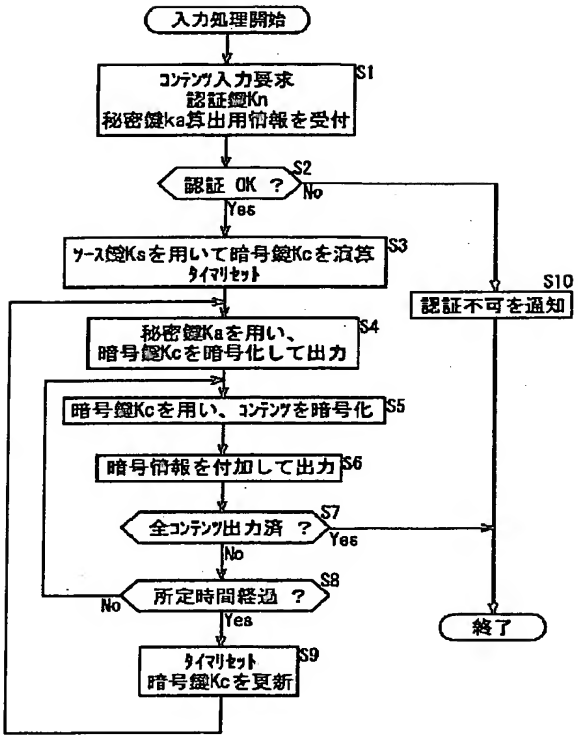
【図４】


41
鍵管理部
暗号情報解析部
暗号化・復号部
コンテンツ処理部
42
43
44
アプリケーション

【図６】


出力処理開始
コンテンツ出力要求
認証鍵Kn
秘密鍵ka算出用情報CCI情報を出力
S21
認証 OK ？
S22
No
Yes
ソース鍵Ksを用いて暗号鍵Kcを演算
S23
S29
認証不可を通知
秘密鍵Kaを用い、
暗号鍵Kcを暗号化して出力
S24
アプリケーションが暗号鍵Kcを用いて
コンテンツを暗号化
S25
暗号鍵Kcを用いてコンテンツを復号
S26
コンテンツをDTLAに基づいて暗号化
S27
出力
S28
終了

【図５】



フロントページの続き

(51) Int. Cl.[7]	識別記号	Ｆ Ｉ	テーマコード（参考）
Ｈ０４Ｌ 9/32		Ｈ０４Ｌ 9/00	６０１Ｅ
			６７３Ｂ

Ｆターム(参考) 5B017 AA06 BA05 BA07 BB02 BB03
BB10 CA07 CA09 CA16
5D044 BC01 CC04 DE17 GK17 HL01
5J104 AA07 AA16 EA04 EA17 KA02
MA02 NA02 NA32 PA14
9A001 BB01 BB03 BB04 BB05 CC05
DD06 EE03 GG22 JJ25 KK37
LL03